Bring Your Own Device

La rete aziendale? Un formaggio coi buchi

A cura di Albert Rodriguez

Il fenomeno del Byod (Bring Your Own Device) si sta diffondendo con rapidità in tutte le organizzazioni. Un numero sempre maggiore di dipendenti ha ormai libero accesso alla rete attraverso dispositivi mobili non aziendali quali tablet e smartphone di ogni marca e modello.
Se da una parte il Byod aumenta la disponibilità delle applicazioni in qualsiasi momento e in qualsiasi luogo – oltre a contribuire a ridurre le spese per gli acquisti di dispositivi It – dall'altra può rivelarsi un fattore che cela una complessità in più per i dipartimenti It, in considerazione della prevenzione dei rischi connessi all'uso di dispositivi diversi da quelli tradizionali. Le nuove applicazioni infatti chiedono alle reti di aumentare l'intelligenza per definire meccanismi specifici, soprattutto in ambito sicurezza.
Non solo le persone accedono dai propri device alla rete aziendale ma, allo stesso modo, utilizzano le applicazioni per scopi personali.
Chi governa tutto questo? Esiste nelle organizzazioni un responsabile della sicurezza preposto alla gestione di tutta questa crescente complessità? La realtà descrive un quadro preoccupante; sono poche infatti le aziende che hanno già implementato policy per la protezione dei dispositivi mobili introdotti nel luogo di lavoro.
Le organizzazioni si stanno rendendo conto che per proteggere le reti e i dati aziendali da potenziali minacce provenienti dai dispositivi mobili è necessario gestire la sicurezza a livello di rete piuttosto che a livello di endpoint.
Le applicazioni mobili rappresentano un 'goloso boccone' per i cyber-criminali, dato il rischio più elevato di attacco rispetto alle applicazioni web. Gli hacker si stanno concen-

Il tavolo dei relatori

trando sempre più sulle applicazioni mobili proprio perché molte organizzazioni non sono consapevoli nemmeno dei rischi per la sicurezza che queste introducono.

Gartner: nel 2016 il budget It supererà quello del marketing

Di tutto questo e – più in generale del problema 'sicurezza It' nelle organizzazioni – si è discusso nel corso di una tavola rotonda che si è tenuta mercoledì 19 settembre all'AC Hotel di Milano. Un'occasione di incontro e di confronto organizzato dalla nostra rivista *Sistemi&Impresa* sostenuta da alcuni dei più importanti player del mercato sicurezza It, quali Akamai Technologies, Fortinet, Novell e SafeNet Italy e che ha inoltre richiamato sette grandi realtà di livello 'enterpise' per discutere delle esperienze e delle esigenze che i dipartimenti It affrontano ogni giorno con l'intrusione sregolata dei device mobili in azienda.

Una pletora di dati allarmanti su questo nuovo trend certo non mancano.

Gartner sostiene che la sicurezza continua a rimanere una delle prime voci ad alta priorità nei budget It e ammonterà a fine anno a 60 miliardi di dollari con un incremento dell'8,4% rispetto allo scorso anno. Si prevede però che la corsa verso la sicurezza arriverà a sfiorare gli 86 miliardi di dollari nel 2016. Tra i Cio intervistati in questa survey di Gartner la metà prevede infatti che il budget per la sicurezza delle infrastrutture It rimarrà invariato, l'altra metà prevede invece una decisa crescita.

Secondo le evidenze di una ricerca condotta da un player del mercato, solo il 54% dei device mobili utilizzati in azienda – e per l'azienda – ha installato un software antivirus, nonostante ben il 40% degli accessi alla intranet avvenga da un device personale. Un fattore che aumenta la probabilità di rischio svela che nella metà casi (46%) l'azienda ancora non ha fornito indicazioni chiare sul da farsi nell'eventualità di gravi rischi per la sicurezza dei dispositivi It.

Anche da una survey condotta a livello globale da Ibm su 130 'Chief information security officer' risulta chiaro come la sicurezza dei dispositivi It e dell'intera rete sia vista come un 'imperativo categorico' per la tutela del business. Secondo Ibm il 60% delle organizzazioni di livello 'enterprise' cita la sicurezza come uno dei primi temi trattati a livello di Consiglio. Le organizzazioni più solide e strutturate tendono a trattare la questione istituendo comitati direttivi per la sicurezza, avendo da tempo compreso la pervasività e la trasversalità del problema.

I buoni comportamenti organizzativi, la prima vera difesa

Comitati di sicurezza, crescita del budget a supporto delle infrastrutture It, stretto monitoraggio della rete: si tratta di possibili argini che tuttavia nulla possono contro la creatività dei cyber-criminali se prima non si interviene sul comportamento delle persone.

Sembra questo il messaggio che aziende e vendor hanno condiviso come un mantra per tutta la durata della tavola rotonda.

"Nessuno garantirà mai una protezione dai malware al 100% se prima non si interviene in termini di formazione e consapevolezza sugli utilizzi accettabili, o impropri, della strumentazione aziendale" esordisce nel suo intervento Andrea Peduto, Hr organization development director di Edison. L'azienda sta muovendo i primi passi per delineare le procedure di policy con l'obiettivo di regolamentare un fenomeno (Byod & Company Mobile Device) che fino ad oggi è stato gestito (in parte) in modo informale. "Non possiamo dimenticare che si tratta di affrontare con velocità sempre crescente un problema di ordine generazionale – prosegue Peduto –. Il fenomeno dei device in azienda comporta assunzioni di rischio maggiori perché i decisori di oggi spesso sono ancora quelli di ieri, ma sono veri e propri neofiti rispetto ai nuovi strumenti, hanno bisogno cioè di più tempo rispetto alle giovani generazioni per prendere confidenza con i vari device, dominarli, non averne paura o non mitizzarli".

Andrea Peduto
Hr organization development director
Edison

Peduto lancia anche un messaggio chiaro ai vendor: siate più rassicuranti e più chiari sul tema sicurezza. Il cambio del modo di lavorare è così veloce oggi che quello che preoccupa di più è l'incapacità di seguire le nuove prospettive.

Le aziende hanno bisogno di ricevere messaggi più chiari.

Franco Michelin
It production director
ADP

Un *claim* molto caro anche a quelle organizzazioni che per la natura stessa del proprio business trattano ogni giorno dati e informazioni ad alta sensibilità, come cedolini paga, residuo ferie, situazione contabile del dipendente. ADP fa proprio questo con i suoi software per la gestione amministrativa del personale. Franco Michelin, It production director, spiega che è il mercato a richiedere l'adozione dei device mobili personali in azienda. Ma le organizzazioni esigono allo stesso tempo la massima tutela, perché – dice Michelin – "Un incidente sulla sicurezza It può mettere a repentaglio per sempre la buona reputazione di un'azienda". ADP ha lanciato

Un momento della tavola rotonda

sul mercato le 'ADP Mobile solutions', si tratta di 'soluzioni mobile' che consentono ai dipendenti di connettersi con la propria organizzazione direttamente da cellulari e tablet attraverso alcune funzionalità 'selfservice' permettendo di visualizzare la propria busta paga, la directory aziendale, la gestione delle assenze (ferie e permessi). "A tale scopo è fondamentale disporre di strumenti che supportino la mobilità" sottolinea Michelin.
Allora sì all'innovazione tecnologica, ma con cautela, muovendo un passo dopo l'altro per la buona riuscita del cambiamento.

Regola numero uno, curare riservatezza e sensibilità del dato

Chi con la massima cautela deve fare i conti tutti i giorni è il mondo bancario, ancora lontano dall'utilizzo della 'nuvola' come repository di dati, ma sempre più interessato alla tecnologia mobile. "Abbiamo già installato *Mobile App* per la clientela dell'internet banking" spiega Luca Fioletti, Responsabile Area Canali della Banca Popolare di Sondrio. L'azienda continua a utilizzare come dispositivo mobile il Blackberry, pur tenendo un occhio di riguardo alle nuove tecnologie smartphone, in particolare Apple e Android.
La sicurezza, secondo Fioletti, si fa sulla App stessa e non sulla rete, come dire: meglio prevenire 'a monte' che curare.

Luca Fioletti
Responsabile area canali
Banca Popolare di Sondrio

Le aziende non hanno solo l'obbligo di proteggere i dati dei propri clienti, spesso hanno la necessità di curare la riservatezza specifica del proprio business, quando questo è unico. È il caso di Pirelli che, fornitore unico di pneumatici per il campionato mondiale di Formula Uno 2011-2013, deve tutelare un know how importante. "Anche perché - racconta Alessandra Banfi, Responsabile della Direzione Information and Communication Technology del Gruppo – "l'azienda è globale, e ciò prevede che buona parte del lavoro sia svolto lontano dall'headquarter, con il rischio di perdere i device contenenti dati sensibili durante gli spostamenti. Per questo stiamo pensando di erogare in futuro delle policy sul tema Byod per permettere a ognuno di usare il proprio device in trasferta garantendo la massima protezione per l'azienda". In tal senso, la direzione It di Pirelli propone di costituire un gruppo di lavoro interfunzionale per definire le 'regole del

Alessandra Banfi
Responsabile Direzione Information and Communication Technology
Pirelli

Pietro de Martino
It security manager
Artsana

L'aperitivo a margine dell'evento

gioco', come ad esempio quello già avviato da Edison. Una di queste regole, che dà alla società il diritto di distruggere i dati aziendali contenuti nel device mobile in caso di perdita, prevede che ciascuno ne sia il diretto responsabile. Resta, invece, da definire la gestione dei dati personali attualmente in fase di valutazione.

Sulla responsabilità personale nella gestione dei device anche Artsana, conosciuta in tutto il mondo per la produzione di medicali come Chicco, Pic, Prénatal, ha già chiara la policy che vuole adottare. "Dei device personali non bisogna abusare in azienda – commenta Pietro de Martino, It security manager. "Tra l'altro – prosegue il responsabile sicurezza It – la linea guida del management è che questi non diventino mai uno *status symbol*, in modo da non abbassare mai il senso del pericolo, creando già in questo modo un 'recinto' per i dati più sensibili". Parrallelamente si sta incoraggiando a un uso virtuoso del device.

Con i device personali l'operatività è al centro del business

Luca Mazzocchi
Infrastructure, Service & Security Manager
Saipem

L'alta mobilità dei dipendenti è l'impronta alla base di un'altra grande organizzazione che vuole sentirsi chiamare 'operativa' e non 'ingessata'. Parliamo di Saipem, società di Eni, con una forte connotazione internazionale. Lavora molto all'estero nell'industria dell'energia: gas e petrolio. L'organizzazione è infatti presente in tutto il mondo con 220 uffici. "È logico che con questa distribuzione i rischi siano evidenti" esordisce Luca Mazzocchi, Responsabile area Ict Security. L'Ict rimane per Saipem un'area a disposizione delle esigenze operative della Corporate, così nel 2011 sono state definite le prime linee guida per definire la gestione dei device per tutto il Gruppo.

È stato così redatto un programma di 'awarness' che, attraverso l'erogazione di sessioni multimediali specifiche per l'utente, mira a far prendere consapevolezza dell'impatto organizzativo che la scelta dell'adozione di un device può avere per l'intero Gruppo. "Siamo già usciti dalla fase pilota – spiega Mazzocchi – ed entrati in quella di produzione. Oggi offriamo servizi ad alto valore aggiunto, come la VPN su iOS, che permette di sfruttare tutti i tool che l'azienda mette a disposizione".

Quando il Byod non vale solo per i dipendenti

Un'altra best practice in tema Byod la offre Auchan, dove da un po' di anni sono state istituite policy per l'accesso ad App specifiche. Nonostante l'azienda fornisca smartphone a dirigenti e direttori dei punti vendita per accedere alla posta e ad alcuni dati aziendali, il Top management preferisce utilizzare il proprio strumento che porta da casa, commenta Marino Vignati, Direttore dei sistemi informativi.

Marino Vignati
Direttore sistemi informativi
Auchan

"L'Ict – dice Vignati – ha inoltre da sempre lavorato a stretto

I Vendor

Akamai

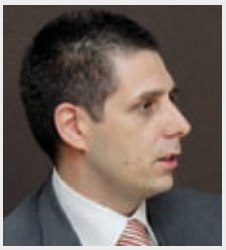
Realtà americana: 1 billion revenue.
Il 20-30% del traffico internet nel mondo passa da tecnologia Akamai. Nell'universo mobile la società statunitense gestisce un business 'verticale', se pensiamo che i più grandi distributori di App al mondo utilizzano Akamai: ogni minuto sono 80.000 le *mobile App* scaricate in tutto il mondo.
A seconda del dispositivo riconosciuto Akamai ottimizza e indirizza la pagina su quel specifico device.
Le parole chiave dell'azienda sono: sicurezza, performance, semplicità, governance centralizzata, definizione di 'Employee exit strategy'. Interventi di 'Security' sviluppati anche contro casi di spionaggio industriale.

Luca Collacciani, Sales Manager Italy

Fortinet

Azienda nata nel 2000 ma già tra i leader di mercato nel 'network security'.
Fortinet caratterizza la sua offerta per la capacità di contenere in un'unica appliance tutte le soluzioni di sicurezza di rete per il monitoraggio di utenti, device e protocolli di rete.
Nel portafoglio della sua offerta si trovano tante funzioni accelerate in hardware che garantiscono un dimensionamento corretto per ogni strumento. Offre dunque un portafoglio completo per qualsiasi tipo di appliance.
L'approccio al Byod è centralizzato a seconda delle App da proteggere. Ciò non toglie che la società sia in grado di definire policy a livello di gruppo, di singolo utente o di device che sta tentando di accedere alla rete.

Antonio Madoglio, System Engineer Manager Italy



Christian Zemella, Systems Engineer

Novell

La sua mission è trasformare il fenomeno emergente del 'Bring your own device' in un vantaggio reale.
La sua arma 'silenziosa' è la protezione del device con la garanzia di snellezza operativa dei processi governati dai sistemi informativi. Lo strumento tecnologico di Novell garantisce la flessibilità necessaria per implementare le policy definite dalle aziende senza costringerle ad adeguare le policy stesse al prodotto scelto. Uno dei punti di forza della sua offerta è una profonda esperienza nella gestione degli endpoint, oggi estesa al mondo del mobile management e del Byod. Obiettivo finale: la gestione completa dell'intero asset aziendale. Per Novell nella gestione del Byod il 'fattore umano' è importante e non può essere sottovalutato; così è fondamentale che per ogni azienda le policy vengano definite a monte di una strategia di utilizzo del device.

SafeNet

Fondata nel 1983, SafeNet, Inc. è una delle principali aziende al mondo nel campo della Information Security ed è riconosciuta per proteggere i dati più sensibili di molte aziende leader di mercato a livello globale. L'approccio data-centric di SafeNet si focalizza sulla protezione delle informazioni ad alto valore durante tutto il loro ciclo di vita, dal data center al cloud e sulla protezione del codice sorgente dei software. Oltre 25.000 clienti tra aziende private e agenzie governative si affidano a SafeNet e alle sue innovative soluzioni crittografiche e di autenticazione forte per proteggere e controllare l'accesso a dati sensibili, ridurre i rischi correlati al trattamento delle informazioni, garantire il rispetto delle normative e rendere sicuri ambienti virtuali e cloud.

Orlando Arena, Regional Sales Director Enterprise

contatto con l'Hr (diritto del lavoro) per definire le policy adeguate all'utilizzo del device e per il monitoraggio della navigazione in rete".
La catena francese è stata tra primi player nel Gdo a consentire anche l'accesso dei clienti alla rete aziendale tramite smartphone, dai quali è già possibile fare la spesa senza uscire di casa. "A Piacenza per esempio – dice Vignati – è più di anno che è attivo questo servizio" (e pare che nella cittadina emiliana siano stati i primi al mondo, primi anche di Walmart). Lo scorso febbraio sono infatti stati premiati a una fiera di settore per questa innovazione.
Nex step: sviluppare anche il processo di pagamento dal device.